HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400
APO AE 09131-0400

DIRECTIVE
NUMBER 25-4 22 October 2002

SECURITY

USEUCOM Policy Guidance for Use of Portable Electronic Devices within Sensitive Compartmented Information Facilities

1. **Summary**. To establish policies and procedures for the possession, use and restrictions pertaining to Portable Electronic Devices (PEDs) within Sensitive Compartmented Information Facilities (SCIFs) under the cognizance of the USEUCOM Director of Intelligence (ECJ2).

2. **Applicability**. This policy is applicable to all SCIFs designated as EUCOM SCIFs by the Defense Intelligence Agency (DIA), Washington, D.C., the US national accreditation authority. This policy is applicable to all USEUCOM personnel (US military, DoD civilian employees and DoD contractor personnel) and all other personnel working within any USEUCOM SCIF. This policy is also applicable to any/all personnel escorted into or visiting within any USEUCOM SCIF.

3. **Internal Control Systems**. This staff directive does not contain internal control provisions and is not subject to the requirements of the internal management control program. For USEUCOM and subordinate joint activities, the applicable internal control directive is ED 50-8, Internal Management Control Program.

4. **Suggested Improvements**. The USEUCOM Department of Defense Intelligence Information System (DoDIIS) Information Systems Security Manager (ISSM) and the USEUCOM Special Security Officer are responsible for this publication. If you have suggestions for improvement, or if you find errors, please contact USEUCOM DoDIIS ISSM, Unit 8845, Box 290, APO AE 09469 or HQ USEUCOM SSO, ATTN: ECJ2-SSO, Unit 30400, APO AE 09131.

5. **References**.

a. DIA Message DTG 031337Z May 02, Subject: Portable Electronic Device (PED) Policy.

b. Information Systems Security Organization (ISSO) Information Assurance (IA) Advisory No. IAA-001-01, Subject: Personal Electronic Devices Security Guidance, dated 16 January 2001.

c. Deputy Secretary of Defense Memo, Use and Protection of Portable Computing Devices, dated 14 July 2000.

d. DCID 1/21, Physical Security Standards for SCI Facilities, 29 July 1994, Annex D, Part 1, Electronic Equipment in SCIFs, approved 20 July 1994.

e. ED 25-2, Security Awareness, Appendix G, Telephone Security, dated 25 January 2001.

6. **Responsibilities.**

a. Commanders, agency heads and supervisors shall be overall responsible for the government PEDs procured for use by their organization and shall support the DoDIIS Site ISSM in the implementation and enforcement of this PED policy.

b. Staff responsible for procurement of government PEDs shall procure only those devices able to meet the minimum requirements of this policy.

c. Users shall:

(1) Adhere to the procedures and requirements outlined in this policy;

(2) Use the government PED for official and approved use only;

(3) Protect the PED from unauthorized access and theft;

(4) Report any violation of this policy to their Site ISSM, ECJ2-SSO, DSN 430-5672/7189 or JAC ISSO/ISSM, DSN 268-2396/2989.

7. **Policy**.

a. Laptops and Notebook Computers

(1) Government Owned:

(a) May be used and carried into or out of SCIFs within the limits of property accountability rules.

(b) **MAY NOT** be connected to any information system without explicit and documented permission from the cognizant Site ISSM. If permission has been obtained and laptops/notebook computers are connected to information systems within a SCIF, documented permission must be maintained by the SCIF Custodian with a copy provided to the cognizant ISSM.

(c) May be approved by the Site ISSM for the use of classified materials.

(d) Must meet minimum technical security requirements for certification and accreditation approval in accordance with applicable directives and regulations.

(e) Laptops and notebook computers with digital audio, video, optical, or optical recording capability are **PROHIBITED** from entry into or use within SCIFs. SCIF Custodians will ensure that systems administrators physically disconnect built in microphones and/or cameras where possible and will disable or remove software drivers for microphones and cameras.

(f) Laptops and notebook computers that have a Radio Frequency (RF) wireless capability are **PROHIBITED** within SCIFs, as reliable countermeasures do not exist to mitigate security risk. Removal of the antenna is not a suitable countermeasure to eliminate RF operations, as some systems can communicate with the antenna physically removed. Therefore, wireless attachments (e.g. network LAN cards and modems) must be removed before the laptop enters the SCIF. If the device is self-powered, the battery must be removed. Where RF capability is mission essential within DIA-accredited SCIFs, the SCIF Custodian must submit a written justification to the Site ISSM. In turn, the Site ISSM may request exceptions through DIA/DAC-2A.

(g) Laptops and notebook computers that have InfraRed (IR) wireless capability or IR ports may be brought into and used within SCIFs. If any of the computer equipment within the facility has IR ports, either the laptop or the facility computer equipment IR port must be disabled (either by software or hardware) while within secure facilities. Simply covering the IR emitter/detector with an opaque tape or other covering is not adequate due to variability in effectiveness and an inability to readily determine the characteristics of the covering by simple visual inspection. Laptops used for processing classified data must have the internal modems physically disconnected and software drivers for modems removed. Personnel responsible for acquiring laptops for processing classified data should make every effort to have them delivered without internal modems. Where IR capability is mission essential within DIA-accredited SCIFs, the SCIF Custodian must submit a written justification to the Site ISSM. In turn, the Site ISSM may request exceptions through DIA/DAC-2A.

(2) Personally Owned:

(a) Personally owned laptop and/or notebook computers are **PROHIBITED** in SCIFs.

(b) There are no exceptions to this policy.

b. Hand-held Devices

(1) Government Owned:

(a) May be used and carried into SCIFs within the limits of property accountability rules.

(b) **MAY NOT** be connected to unclassified information systems without the explicit and documented permission of the Site ISSM. The Site ISSM may approve the connection of government owned hand-held devices to unclassified information systems on a case-by-case basis.

(c) Hand-held devices **ARE NOT APPROVED** for the use of classified materials or for connection to classified information systems.

(d) Hand-held devices, to include Personal Digital Assistants (PDAs) with audio, video, or optical record capability are **PROHIBITED** from entry into or use within SCIFs. Government owned cameras (i.e. optical/video recording devices) within EUCOM SCIFs must be approved in advance by the SSO on a case-by-case basis IAW DCID 6/9 restrictions (e.g. for official functions). In SSO-approved cases, the area must be appropriately sanitized before any kind of audio, video, optical, or digital recording takes place. All associated media will be controlled.

(e) Hand-held devices that have RF wireless capability are **PROHIBITED** within SCIFs, as reliable countermeasures do not exist to mitigate security risk. Removal of the antenna is not a suitable countermeasure to eliminate RF operations, as some systems can communicate with the antenna physically removed. Where RF capability is mission essential within DIA-accredited SCIFs, the SCIF Custodian must submit a written justification to the Site ISSM. In turn, the Site ISSM may request exceptions through DIA/DAC-2A.

(f) Hand-held devices that have IR wireless capability or IR ports may be brought into and used within SCIFs. If any of the computer equipment within the facility has IR ports, either the handheld device or the facility computer equipment IR port must be disabled (either by software or hardware) while within secure facilities. Simply covering the IR emitter/detector with an opaque tape or other covering is not adequate due to variability in effectiveness and an inability to readily determine the characteristics of the covering by simple visual inspection. Where IR wireless or IR ports are mission essential within DIA-accredited SCIFs, the SCIF Custodian must submit a written justification to the Site ISSM. In turn, the Site ISSM may request exceptions through DIA/DAC-2A.

(2) Personally Owned:

(a) May be used and carried into SCIFs. The Site ISSM and/or Special Security Officer (SSO) shall develop a process/procedure for controlling and recording hand-held devices and for the physical control of approved personally owned hand-held devices used and carried in or out of the Site's SCIFs (e.g., barcode scanning, labeling, database registration, letters of authorization, delegation to SCIF Custodians, etc.)

(b) **MAY NOT** be connected to information systems.

(c) **ARE NOT APPROVED** for the use of classified materials.

(d) Hand-held devices with audio, video, optical, or digital record capability are **PROHIBITED** from entry into or use within SCIFs.

(e) Hand-held devices that have a RF wireless capability are **PROHIBITED** within SCIFs, as reliable countermeasures do not exist to mitigate security risk. Removal of the antenna is not a suitable countermeasure to eliminate RF operations, as some systems can communicate with the antenna physically removed.

(f) Hand-held devices that have IR wireless capability or IR ports may be brought into and used within SCIFs; however the wireless capability may not be used due to technical security risks.

c. Cellular Telephones

(1) <u>Government Owned</u>:

(a) Government owned cellular telephones are **PROHIBITED** from use or being carried into or out of SCIFs due to technical security risks.

(b) Cellular telephones, radios, or other two-way communication devices are **PROHIBITED** from use in any USEUCOM areas where sensitive or classified discussions and processing take place.

(2) <u>Personally Owned</u>:

(a) Personally owned cellular telephones are **PROHIBITED** from use or being carried into SCIFs due to technical security risks.

(b) Cellular telephones, radios, or other two-way communication devices are **PROHIBITED** from use in SCIFs.

d. **Pagers**:

(1) <u>Government Owned:</u>

(a) Receive-only pagers may be used and carried into or out of SCIFs within the limits of property accountability rules.

(b) Two-way pagers are **PROHIBITED**.

(c) Pagers with audio, video, optical, or digital record capability are **PROHIBITED** from entry into or use within SCIFs.

(2) Personally Owned:

(a) Receive-only pagers may be used and carried into or out of SCIFs.

(b) Two-way pagers are **PROHIBITED**.

(c) Pagers with audio, video, optical, or digital record capability are **PROHIBITED** from entry into or use within SCIFs.

e. All PEDs used within SCIFs must meet minimum security requirements, as outlined in this policy and applicable references.

f. PEDs must be physically protected at all times. The entry and exit of PEDs into and out of SCIFs must be closely monitored. The local ISSM and/or SCIF Custodian shall develop procedures for control of government-owned PEDs used by deployed or traveling personnel.

g. All policy regarding the government-owned PEDs shall also apply to contractor business-owned PEDs. The use of PEDs by contractor personnel shall be stated in the contract as mission essential, and are subject to the conditions above for government procured PEDs. Additionally, the use of government purchased/provided PEDs must be identified in the Statement of Work or elsewhere in written agreements between the company and the US government.

h. Any PEDs, approved for unclassified use only, which may inadvertently record, receive, transfer, or connect to a government system, containing classified information, will be considered classified and will be confiscated.

i. Use of commercially procured encryption systems (i.e. CryptoGram, zixmail, etc.) for classified information on government-owned PEDs or media is prohibited. NSA approved encryption must be used.

j. PEDs are subject to random inspection by ISSM, SSO or Command Personnel to ensure appropriate use and compliance with this policy. Personally owned PEDs with encrypted information are subject to confiscation until a determination is made concerning the classification of the material contained therein.

k. Any violation of this policy will be reported to the local security authorities as a security incident, and investigated accordingly.

8. **Disclaimer**. Nothing in this document shall relieve an individual of the responsibility to ensure proper security measures are implemented. Additionally, the guidance provided applies to technology available at the time of publication only. New developments in technology and/or capabilities not specifically addressed in this document shall require further implementing guidance. Without that guidance, users must not presume these devices are approved for use within SCIFs.

9. **Exceptions**. Requests for exception to policy must be addressed in writing through the USEUCOM DoDIIS ISSM and the USEUCOM Special Security Officer (SSO).

FOR THE COMMANDER:

OFFICIAL:

DANIEL J. PETROSKY
Lieutenant General, USA
Chief of Staff

AVA N. WEBB-SHARPLESS
Lt Col, USAF
Adjutant General

DISTRIBUTION:
P